UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,033	12/31/2003	Carlos J. Gonzalez	SNDK.281US0	3703

66785 7590 09/18/2007

DAVIS WRIGHT TREMAINE LLP - SANDISK CORPORATION
505 MONTGOMERY STREET
SUITE 800
SAN FRANCISCO, CA 94111

EXAMINER	
MASKULINSKI, MICHAEL C	
ART UNIT	**PAPER NUMBER**
2113	

MAIL DATE	DELIVERY MODE
09/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/751,033
Filing Date: ***
Appellant(s): GONZALEZ ET.AL

Gerald Parsons
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 17, 2007 appealing from the Office action mailed January 19, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2004/0205328 A1	Langford et al.	10-2004
US 2004/0088534 A1	Smith et al.	5-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4, 10, 17, 18, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Langford et al., US 2004/0205328 A1, and further in view of Smith et al., US 2004/0088534 A1.

Referring to claim 1:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (flash memory containing at least first and second copies of firmware code stored in different locations therein). Further, in paragraphs 0018 and 0020, Langford et al. disclose a microprocessor, a read-only-memory (ROM) containing microprocessor accessible boot code and a random-access-memory (RAM) for storing microprocessor accessible firmware code.

b. In paragraph 0027, Langford et al. disclose that when boot code is executed within the memory, the boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid. The validity flag is stored in a nonvolatile memory. Further, in paragraph 0038, Langford et al. disclose that the validation may take the form of a cyclical redundancy check across the entire image (executing the boot code to transfer a first copy of the firmware from the flash memory to the RAM, identifying any bit errors in the transferred first copy of the firmware code).

c. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the

validation may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose that if bit errors are identified that are correctable, correcting the erroneous bits. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

d. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image (if bit errors are identified that are not correctable, reading at least a portion of the second copy of the firmware code into the RAM in place of at least a portion of the first copy containing the uncorrectable bit errors, and executing an error free copy of the firmware code from the RAM).

Referring to claim 2, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to

be able to correct at least single bit errors with the error correction codes (wherein identifying any bit errors in the transferred first copy includes calculating error-correction-codes (ECCs) from individual portions of the first copy of the firmware by passing the firmware portions through ECC circuitry in succession as they are being transferred from the flash memory to the RAM, and comparing the calculated ECCs with ECCs previously calculated from said portions of the first copy of the firmware data).

Referring to claim 3, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes. Since Smith et al. disclose error correction codes; it would be inherent to the system of Smith et al. to microprocessor executing an error correction algorithm of the boot code to correct erroneous bits.

Referring to claim 4, in paragraph 0047, Smith et al. disclose data elements within BIOS code and corresponding error correction codes associated with the BIOS code (wherein the individual portions of the first copy of the firmware code include one or more sectors of data and an ECC previously calculated therefrom and stored in the flash memory therewith).

Referring to claim 10, in paragraph 0047, Langford et al. disclose that when boot code is executed within memory, boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid (prior to executing the boot code to transfer a first copy of the firmware from the flash memory to the RAM, checking the state of a firmware present flag that is set when firmware is stored in the

flash memory and continuing to execute the boot code to transfer the first copy of the firmware from the flash memory to the RAM only when the firmware present flag is set).

Referring to claim 17:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (flash memory containing at least first and second copies of firmware code stored in different addressable locations). Further, in paragraphs 0018 and 0020, Langford et al. disclose a microprocessor, a read-only-memory (ROM) containing microprocessor accessible boot code and a random-access-memory (RAM) for storing microprocessor accessible firmware code.

b. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose storing at least first and second copies of firmware code in different addressable locations of the flash memory by passing the firmware copies one at a time through the ECC circuitry and storing the ECCs calculated thereby in the flash memory. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are

commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

c. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation (thereafter initiating operation of the memory system by causing the microprocessor to execute the boot code to transfer the first copy of the firmware from the flash memory to the RAM) and it would be inherent to the system of Smith et al. to be able to calculate an ECC when transferring data to the RAM.

d. It would be inherent to the combined system of Langford et al. and Smith et al. to utilize the calculated and stored ECCs to identify any bit errors in the transferred first copy of the firmware code, and if bit errors are identified to be correctable, causing the microprocessor to execute an error correction algorithm within the boot code to correct the erroneous bits, in order to result in the firmware code being loaded into the RAM without any errors.

e. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image (if bit errors are identified to be uncorrectable,

transferring at least a portion of the second copy of the firmware code into the RAM in place of at least a portion of the first copy containing the uncorrectable bit errors, in order to result in the firmware code being loaded into the RAM without any errors).

Referring to claim 18, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes (wherein storing the firmware code includes storing ECCs individually calculated from one or more sectors of the firmware code).

Referring to claim 20, in paragraph 0047, Langford et al. disclose that when boot code is executed within memory, boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid and in paragraph 0028, Langford et al. disclose that if on the other hand, Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system from the other firmware image (wherein storing the firmware code additionally includes setting a flag to indicate the presence within the flash memory of at least one firmware copy, and wherein executing the boot code to transfer either of the first or second copies of the firmware code includes first reading the flag associated therewith and proceeding to read the copy of the firmware code only if the associated flag is set).

Referring to claim 23:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (an array of flash memory cells storing data in charge storage elements and containing at least first and second

copies of firmware code therein). In paragraphs 0027 and 0038, Langford et al. disclose that the validation of data may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose having first and second sets of error-correction codes (ECCs) calculated from the first and second copies of the firmware code. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

b. In Figure 2, Langford et al. disclose a controller processor.

c. Circuitry that calculates ECCs from data passing through the circuitry would be inherent to Smith et al. since Smith et al. has ECCs.

d. Further, in paragraphs 0018 and 0020, Langford et al. disclose a read-only-memory containing boot code that the processor accesses and executes in response to initialization of the storage system and a random-access-memory that is accessible by the processor to obtain instructions to be executed.

e. In paragraph 0027, Langford et al. disclose that when boot code is executed within the memory, the boot code will check a flag, such as Pside

validity flag to determine whether the image within Pside flash memory is valid. The validity flag is stored in a nonvolatile memory. Further, in paragraph 0038, Langford et al. disclose that the validation may take the form of a cyclical redundancy check across the entire image (wherein the boot code causes the processor to read the first firmware code copy including passing the read first firmware code copy through the ECC calculation circuitry which calculates ECCs and provides with respect to the first set of ECCs stored with the first firmware code copy a status with respect to any data errors existing in portions of the first firmware code copy to which the ECCs pertain).

f. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation ((A) if the status indicates that there are no data errors in a given Art Unit: 2113 one of the portions of the first firmware code copy, thereafter writing the given portion of the first copy of the firmware code into the random-access-memory).

g. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes ((B) if the status indicates that there are data errors in the given portion of the first firmware code copy, the boot code causes the processor to determine whether the number of bit errors in the firmware code exceed a given number, and (i) if the number of bit

errors do not exceed the given number, further causes the processor to correct the erroneous bits and write the corrected first firmware code copy into the random-access-memory).

h. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image ((ii) if the number of bit errors is equal to or exceeds the given number, further causes the processor to read at least a portion of the second firmware copy).

i. In paragraph 0028, Langford et al. disclose that if, on the other hand, Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system from the other firmware image. In this example, boot loader will check Tside validity flag for Tside flash memory. If this flag is valid, boot code will continue to boot the data processing system using the images located in this flash memory (pass the read second firmware code through the ECC calculation circuitry which calculates at least one ECC therefrom and provides a status with respect to any data errors existing in said at least a portion of the second firmware code copy to which said at least one ECC pertains, and if the status indicates that there are no data errors in said at least one portion of the second firmware code copy, thereafter writing said at least one portion of the read second copy of the firmware code into the random-access-memory).

(10) Response to Argument

On page 5, under the section Summary, the Appellant argues, "But rather than check for data errors during the uploading (booting) of the boot code from that memory, as included in the appealed claims for uploading firmware into a memory system, the validity of the code is determined when it is downloaded into the memory and a flag is stored with each copy to indicate whether it is valid. When uploading the boot code during initialization of the data processing system, Langford et al. checks this flag of one of the code copies before transferring that copy from the non-volatile memory into operating memory of the data processing system. No validity check or error correction is described by Langford et al. to be performed during this uploading, contrary to the process of the appealed claims. The Examiner disagrees. Regarding the reference of Langford et al. and the Appellant's claim language, in paragraph 0025 Langford et al. disclose that boot code 300 is loaded into memory 302 when a data processing system, such as data processing system 200 is booted or initial program load begins. Memory 302 may be, for example, FSP DRAM 221 in FIG. 2. In this example, boot code 300 is a copy of boot code 304, which is located in Pside flash memory 306. This citation teaches the Appellant's claim language of "executing the boot code to transfer a first copy of the firmware from the flash memory to the RAM." In paragraph 0027, Langford et al. continue by disclosing that when boot code 300 is executed within memory 302, boot code 300 will check a flag, such as Pside validity flag 320 to determine whether the image within Pside flash memory is valid. Validity flag 320 is stored in a non-volatile memory. This citation teaches Appellant's claim language of "identifying any bit errors

in the transferred first copy of the firmware code". The Examiner respectfully believes that the Appellant's statement is in error because according to the citations and flow of Langford et al., the boot code is loaded from the flash 306 into DRAM memory 302 and then the Pside flag is checked.

On page 7, under the section, The Langford et al. Reference, the Appellant argues, "Langford et al. clearly want to avoid beginning to load a copy of the boot code if any portion of it is invalid. 'In this manner, boot time is saved from preventing the computer system from booting from a defective firmware image until an error is encountered and then having to begin the boot process again using a redundant image.' (Langford et al. 0029, lines 1-4). Langford et al. saves this boot time by not beginning to upload a copy of the boot code until it is determined that its stored validity flag (Pside or Tside) indicates that the data of the copy are valid." The Examiner disagrees. The Appellant's argument is nothing more than speculation because the citation relied upon never states when the validity flag is checked.

On page 7, under the section, The Langford et al. Reference, the Appellant argues, "If there are bit errors and they are correctable, they are corrected. If uncorrectable, at least some of the second firmware copy is loaded in place of at least the portion of the first copy containing the uncorrectable bit errors. There is no suggestion or mention by Langford et al. of the claimed identification and correction of erroneous boot data bits in the uploading process or reliance on the second firmware copy if the errors cannot be corrected. Loading of boot code will not be commenced unless its validity flag indicates that there are no bit errors in the stored code." The

Examiner disagrees. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image (if bit errors are identified that are not correctable, reading at least a portion of the second copy of the firmware code into the RAM in place of at least a portion of the first copy containing the uncorrectable bit errors, and executing an error free copy of the firmware code from the RAM). Further, the Examiner has never relied on Langford et al. to disclose correcting of erroneous boot data bits.

On page 7, under the section, The Smith et al. Reference, the Appellant argues, This paragraph merely mentions that when BIOS (basic input-output system) code is updated, a corresponding checksum or error correction code is also updated. The same disclosure is repeated in paragraph 0052 (lines 11-14) of Smith et al. Other than these two mentions, nothing can be found in Smith et al. that discusses checksums or error correction codes or their use." The Examiner disagrees. Because Smith et al. teach storing an error correction code, it is inherent to the reference of Smith et al. to use the error correction code to correct the errors. That is the whole point of storing an error correction code in a memory.

On page 7, under the section, The Smith et al. Reference, the Appellant argues, "It is submitted that Smith et al. would not have made it obvious to correct erroneous bits of the first copy of the boot code of Langford et al. with an error correction code as the boot code is being transferred out of non-volatile memory into RAM. Nor would Smith et al. have made it obvious to then, if the first copy cannot be corrected, to load at

least some portion of the second copy." The Examiner disagrees. Langford et al. teach checking a validity flag after loading the boot code into RAM. Smith et al. teach the storage of error correction codes with the boot code (BIOS). It would have been obvious to one of ordinary skill in the art to combine the error correction capability of Smith et al. with the error detection step of Langford et al. because it prevents the unnecessary use of the second boot code when the errors can be corrected with error correction codes. In other words, Smith et al. improves the system of Langford et al. by making it more fault tolerant to small bit errors. Further, the Examiner has never relied on Smith et al. to disclose that if the first copy cannot be corrected, to load at least some portion of the second copy.

On page 8, under the section, The Smith et al. Reference, the Appellant argues, "It is further submitted that Langford et al. expressly teach against making any such modification by stressing the importance of determining the validity of a boot code copy before any loading of it into system RAM is allowed to begin. 'The mechanism of the present invention saves on boot time by preventing a computer system from booting from a defective image and then having to switch to another image after the defective portion of the defective image has been encountered.' (Langford et al. 0040, lines 1-4). » The Examiner disagrees. This citation never states that the boot code is checked before loading it into RAM. Further, it supports the obvious combination because the correction of errors saves on boot time by preventing a computer system from booting from a defective image.

On page 8, under the section, The Smith et al. Reference, the Appellant argues, "Langford et al. certainly do not suggest switching from transferring from one code copy to the other. To the contrary, Langford et al. stress not having to switch between two copies, as quoted in the preceding paragraph." The Examiner disagrees. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image. Clearly Langford et al. switch to another boot copy. Further, the Examiner would like to note that Langford et al. disclose continuing to boot from the other firmware image and not restarting the boot from the other firmware image. This teaches reading at least a portion of the second copy of the firmware code into RAM in place of at least a portion of the first copy containing the uncorrectable bit errors

On page 8, under the section, The Smith et al. Reference, the Appellant argues, "Smith et al. would certainly not have suggested, by its mere mention of updating error correction codes, that the operation of Langford et al. should be modified in a manner contrary to its expressed goals." The Examiner disagrees because Langford et al. has never taught that error correction codes should not be used. In actuality, Langford et al. support the use of error correction codes by stating a goal is to prevent booting from a corrupted image.

3. On page 11, under the section **REMARKS**, the Applicant argues, "This appears to be based solely on the mention by Smith et al. of use of correction codes. It is

respectfully submitted that this would not have suggested that the first copy of the boot code of Langford et al. be corrected before there is loading of the second copy, which is what is claimed. This is much more than what is mentioned by Smith et al." The Examiner respectfully disagrees. Smith et al. is relied upon to teach error correction codes and the correction of errors. Obviously if the errors of Langford et al. were corrected using Smith et al., there would not be any need to load a second copy. The Applicant is reminded that the references are considered as a combination and that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

4. On page 11, under the section **REMARKS**, the Applicant argues, "Further, Langford et al. expressly teach against the making of such a modification by stressing the importance of determining the validity of a boot code copy before any loading of it into system RAM is allowed to begin." The Examiner disagrees. As stated above this assertion is incorrect and is not disclosed by Langford et al.

5. With respect to the arguments regarding claims 17 and 23, the Examiner respectfully disagrees at least for the reasons above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael Maskulinski

Michael Maskulinski

Conferees:

Scott Baderman

Robert Beausoliel